UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/741,668	12/19/2000	Akira Nonaka	09812.0497-00000	7062

22852 7590 05/01/2009

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER	
DAVIS, ZACHARY A	
ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
05/01/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/741,668	NONAKA ET AL.	
	Examiner	Art Unit	
	Zachary A. Davis	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 April 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,5,7-11,15-22 and 57* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,5,7-11,15-22 and 57* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 13 April 2009 has been entered.

2. By the above submission, Claims 1, 17, and 57 have been amended. No claims have been added or canceled. Claims 1-3, 5, 7-11, 15-22, and 57 are currently pending in the present application.

Response to Arguments

3. Applicant's arguments filed 13 April 2009 have been fully considered but they are not persuasive.

Claims 1-3, 5, 7-11, and 15-17 were rejected under 35 U.S.C. 103(a) as unpatentable over Schneier et al, US Patent 5768382, in view of Christiano, US Patent 5671412, Stefik et al, US Patent 5629980, and Peinado et al, US Patent 7103574. Claims 18-22 were rejected under 35 U.S.C. 103(a) as unpatentable over Schneier in

view of Christiano, Stefik, and Peinado, and further in view of Castor et al, US Patent 5590288. Claim 57 was rejected under 35 U.S.C. 103(a) as unpatentable over Christiano in view of Stefik and Peinado.

In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

Specifically, with reference to the above rejections in general and with specific reference to independent Claim 1, Applicant argues that Peinado does not disclose generating hash values of content key data or usage control policy data by compressing the data into data having a predetermined bit length and that any signature data in Peinado is not created using such hash values (see pages 13-14 of the present response). The Examiner respectfully disagrees. It is clear from the cited portions of Peinado that the digital signature which is included within the license described therein is a digital signature on at least the content decryption key and the usage control data (see column 2, lines 57-64 and column 20, line 38-column 21, line 21, especially column 20, lines 59-62, where the signature is explicitly described, the decryption key KD corresponds to the content key, and the license DRL which includes rights descriptions and/or terms and conditions of the license clearly corresponds to the usage control data). It is well known that a digital signature can be created first by generating hash values of the data to be signed, and then performing public key encryption on those

hash values. See also Schneier, column 9, line 40-column 10, line 56, describing digital signatures as well known in the art, and also Peinado, column 28, line 1-column 30, line 36, showing sample licenses, noting more specifically column 28, lines 57-64, and column 29, lines 38-45, showing the signatures of the respective sample licenses, and column 30, lines 22-36, describing fields of the signatures including the hash algorithm and signature algorithms used. Further with respect to the newly added limitation that hash values are generated by compressing data to a predetermined bit length, the Examiner submits that it is also well known that, by definition, a hash function generates its hash values by compressing the data to a predetermined bit length. See also Schneier, column 49, lines 18-27, explicitly defining hash functions, and also column 9, lines 40-58, more generally describing one way hash functions ("also known as compression functions") as well-known; see further column 17, line 64-column 18, line 30, describing specific hash algorithms, such as SHA, MD4, and MD5, which each have specific predetermined output bit lengths, and also describing in more detail an example hash function that compresses data to a predetermined bit length. See also Peinado, column 28, line 1-column 30, line 36, showing sample licenses, noting more specifically column 28, line 59, and column 29, line 40, showing the hash algorithms used in the respective sample licenses, and column 30, lines 31-32, describing fields of the signatures including the hash algorithm, noting that the example of MD5 has a specific predetermined output bit length (namely 128 bits).

Therefore, the Examiner submits that Peinado does disclose a hash value generating circuit that generates hash values of the content key and policy data and a

public key encryption circuit that creates and verifies signature data using the hashes (again, see Peinado, column 2, line 65, and column 20, line 38-column 21, line 12, as previously cited), and this in combination with the disclosures of Schneier, Christiano, and Stefik renders obvious the claimed invention (see, for example, Schneier, column 9, lines 40-61, column 17, lines 46-50, disclosing generation of hash values of content data, and column 10, lines 41-56 that further disclose a public key encryption circuit creating signature data using hash values of the content data and verifying the integrity of the signature data; see also Stefik, column 26, line 65-column 27, line 9, and column 51, lines 9-12, generally disclosing public key encryption circuits creating signature data, all as previously cited). In particular, it is noted that it would be obvious to modify the disclosures of, for example, Schneier, that teach generating hash values and signature data of content data (again, see Schneier, column 9, lines 40-61; column 17, lines 46-50; and column 10, lines 41-56) to also generate hash values and signature data based on the key and usage policy data as taught by Peinado (again, see Peinado, column 2, line 65; and column 20, line 38-column 21, line 12) in order to maintain the integrity of all of those items and prevent alteration of the key or usage policy data and/or prevent unauthorized decryption of content (again see Peinado, column 25, lines 53-59; see also Schneier, column 9, line 40-column 10, line 67). It is additionally noted that the disclosure of Peinado at least suggests, in itself, that hash values and signature data are also generated from the content itself (noting column 25, lines 41-59, where the signature validation also prevents alteration of the digital content, thus at least suggesting that the digital content can be signed as well).

It is again noted that the present claims do not specify that all of the items (content data, content key, and usage control policy data) are combined into a single hash value or signature (noting that the language of Claim 1, for example, only specifies that the circuit "generates hash values", plural) and therefore the generation of separate hash values of the content data, as in Schneier (as cited above), and of the key and usage policy data, as in Peinado (as cited above), is seen to be sufficient disclosure of the claimed limitations of generation of hash values of the content data, content key, and usage control policy data and the creation of signature data using those hash values (see, for example, Claim 1). The Examiner further notes that Applicant's arguments largely amount to allegations because no specific evidence or detailed explanation appears to have been relied upon in support of the above arguments (see pages 13-15 of the present response).

Therefore, for the reasons detailed above, the Examiner maintains the rejections as set forth below.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 1-3, 5, 7-11, 15-22, and 57 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Each of Claims 1, 17, and 57 has been amended to recite "compressing the data into data having a predetermined bit length". The antecedent basis for the limitation "the data" is unclear because the claims each previously referred to content data, content key data, and usage control policy data, and it is not explicitly clear to which of these data the term is intended to refer. For purposes of interpreting the prior art, the phrase has been assumed to be intended to refer to each of the above data items (and potentially more generic data as well).

Claims not specifically referred to above are rejected due to their dependence on a rejected base claim.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1-3, 5, 7-11, and 15-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier et al, US Patent 5768382, in view of Christiano, US Patent 5671412, Stefik et al, US Patent 5629980, and Peinado et al, US Patent 7103574.

In reference to Claim 1, Schneier discloses an apparatus within a tamper-resistant circuit module (column 8, lines 17-27; column 11, lines 31-37) including a first bus (see Figures 4C-4H); an arithmetic processing circuit (Figure 4C, CPU 302); a

storage circuit (Figure 4C, ROM 304); a second bus (see Figures 4C-4H); an interface circuit (see Figure 4C); an encryption processing circuit (Figure 4B-4C, encryption/decryption module 28; also column 11, lines 41-46); a hash value generating circuit that generates hash values of content data (column 9, lines 40-61; column 17, lines 46-50); a public key encryption circuit (column 10, lines 27-56) that creates signature data using hash values and verifies the integrity of the signature data (column 10, lines 41-56; column 9, lines 40-61); a common key encryption circuit (column 9, line 62-column 10, line 11); and an external bus interface circuit (Figure 4C, I/O 312). However, Schneier does not explicitly disclose determining a mode based on a handling policy and creating log data, nor does Schneier disclose creating usage control status data or controlling the use of the content data.

Christiano discloses determining a usage or purchase mode based on a usage license policy (column 6, line 60-column 7, line 30) and logging data (column 18, lines 53-61), where the log data includes a unique identifier of content data (column 18, lines 53-61), discount information (column 17, lines 35-54, and column 18, lines 53-61), and tracing information (column 18, lines 53-61, and column 6, line 60-column 7, line 46). Christiano further discloses creating usage control status data (column 10, lines 53-57) that includes a content identification (column 10, lines 27-33), the purchase mode (column 10, line 53-column 11, line 11), identification of a circuit module (column 10, lines 33-36), and a user identification (column 10, lines 53-57; column 6, lines 64-column 7, line 1; column 4, line 61-column 5, line 2). Christiano additionally discloses controlling use of content data (column 10, line 64-column 11, line 3) and a usage

monitor that monitors the usage control policy and status data to ensure that content data is properly used based on a license (column 6, line 60-column 7, line 46; column 10, lines 53-57). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the apparatus of Schneier by including the usage policies and licensing as disclosed by Christiano, in order to provide a variety of options and flexibility in controlling usage of licensed data (see Christiano, column 3, lines 12-19).

Although Schneier and Christiano disclose a purchase mode (see Christiano, column 10, line 53-column 11, line 11), neither Schneier nor Christiano explicitly discloses that the purchase mode is determined from one or more purchase mode options, each having a different level of restriction imposed on a playback operation. Stefik discloses a system for controlling distribution and use of digital works that includes a plurality of purchase modes (see Stefik, column 17, line 63-column 26, line 35; more specifically, see column 17, line 64-column 18, line 6; column 19, lines 20-31, describing limitations on number of copies, fees, and times; column 19, lines 46-57, where rights defining playing and printing of a work are described; column 21, lines 10-24, defining limitations on a number of copies to be made; see also column 43, line 45-column 50, line 14, defining various use scenarios) each having a different level of restriction imposed on a playback operation (see again column 17, line 63-column 26, line 35, for a variety of rights, and column 43, line 45-column 50, line 14, for a variety of use scenarios; see also column 36, lines 30-64, where limitations are checked for a playback operation). Stefik also discloses generating log data (column 34, lines 25-34),

where the data can include a unique identifier of the content data (column 9, lines 56-66, and Figure 7), discount information (Stefik, column 23, line 44-column 25, line 8), and tracing information (column 48, lines 20-26), and the data can further indicate a result of the determined mode (see again column 17, line 63-column 26, line 35, and column 43, line 45-column 50, line 14, noting, in particular, for example, column 45, lines 33-47). Stefik additionally discloses a public key encryption circuit (column 26, line 65-column 27, line 9) that creates signature data (column 51, lines 9-12), and also discloses a common key encryption module (column 42, lines 6-21). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the apparatus of Schneier and Christiano by including a plurality of purchase modes each imposing different restrictions on playback, in order to allow the owner of a digital work to attach to the work usage rights defining how the work may be used and/or distributed (see Stefik, column 3, lines 51-61).

Further, although Schneier, Christiano, and Stefik disclose a hash value generating circuit that generates a hash value of content data (Schneier, column 9, lines 40-61; column 17, lines 46-50), none of Schneier, Christiano, or Stefik explicitly discloses also generating a hash value of the key data and usage control policy data. Peinado discloses a system in which a license for digital content includes the content key and usage control policy data (column 2, lines 57-64) and that has a hash value generating circuit that generates a hash value of the content key and policy data and a public key encryption circuit that creates and verifies signature data using the hash (column 2, line 65; column 20, line 38-column 21, line 12). Therefore, it would have

been obvious to one of ordinary skill in the art at the time the invention was made to further modify the apparatus of Schneier, Christiano, and Stefik, to also compute a hash and generate a signature based on the key and usage policy data, in order to maintain the integrity of those items and prevent alteration of the key or usage policy data and/or prevent unauthorized decryption of content (see Peinado, column 25, lines 53-59) as is well known in the art (see also Schneier, column 9, line 40-column 10, line 67).

In reference to Claim 2, Schneier as modified above further discloses a second interface circuit and that the first bus includes a third bus and a fourth bus (see Schneier, Figures 4C-4H).

In reference to Claim 3, Schneier as modified above further discloses a third interface circuit communicating with a recording medium (see Schneier, Figure 4H, interface circuitry 406), a fifth bus, and a fourth interface circuit (see Schneier, Figures 4C-4H).

In reference to Claim 5, Schneier as modified above further discloses that the storage circuit stores private and public key data (see Schneier, column 11, lines 44-48), the public key encryption circuit verifies the integrity of signature data and creates signature data (see Schneier, column 10, lines 41-56; Stefik, column 51, lines 9-12; Peinado, column 2, line 65, for example), and the common key encryption circuit encrypts and decrypts content data and key data using a session key (Schneier, column 9, line 65-column 10, line 6; Stefik, column 42, lines 6-21).

In reference to Claim 7, Schneier as modified above further discloses a random number generating circuit (see Schneier, column 10, lines 57-67).

In reference to Claim 8, Schneier as modified above further discloses an external storage circuit (see Schneier, column 7, lines 57-60).

In reference to Claims 9 and 11, Schneier as modified above discloses everything as applied to Claim 8 above. Schneier as modified above further discloses that programs are executed from memory in a conventional manner (see Schneier, column 7, lines 60-61). However, neither Schneier, Christiano, Stefik, nor Peinado explicitly discloses a storage-circuit control circuit or a storage management circuit. Official notice is taken that it is well known in the computer arts to include a memory controller or memory management circuit, such as a DMA or MMU, in order to allow for the optimization of the use of memory. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the apparatus of Schneier, Christiano, Stefik, and Peinado by including a memory controller or manager, in order to optimize the use of memory, as is well known in the computer arts.

In reference to Claim 10, Schneier as modified above further discloses that the external bus is connected to a host processor (see Schneier, Figure 4C, where the I/O 312 is connected to external CPU 27).

In reference to Claim 15, Schneier as modified above further discloses further disclose a real time clock (see Schneier, column 11, line 46). Further, Schneier, Christiano, and Stefik disclose encrypting key data and control data (see Christiano, column 14, lines 23-28) and storing license key data (Christiano, column 14, lines 19-21).

In reference to Claim 16, Schneier as modified above further discloses further disclose that the storage circuit writes and erases data in units of blocks and also discloses a write lock control circuit for controlling writing and erasing blocks of data (see Schneier, column 18, lines 39-43).

In reference to Claim 17, Schneier discloses an apparatus within a tamper-resistant circuit module (column 8, lines 17-27; column 11, lines 31-37) including a first bus (see Figures 4C-4H); an arithmetic processing circuit (Figure 4C, CPU 302); a storage circuit (Figure 4C, ROM 304); a second bus (see Figures 4C-4H); an interface circuit (see Figure 4C); an encryption processing circuit (Figure 4B-4C, encryption/decryption module 28; also column 11, lines 41-46); a hash value generating circuit that generates hash values of content data (column 9, lines 40-61; column 17, lines 46-50); a public key encryption circuit (column 10, lines 27-56) that creates signature data using hash values and verifies the integrity of the signature data (column 10, lines 41-56; column 9, lines 40-61); a common key encryption module (column 9, line 62-column 10, line 11); and an external bus interface circuit (Figure 4C, I/O 312). Schneier further discloses receiving an interrupt from an external circuit, performing processing, and reporting a result of the processing (column 11, lines 55-67). However, Schneier does not explicitly disclose determining a mode based on a handling policy and creating log data, nor does Schneier disclose creating usage control status data or controlling the use of the content data.

Christiano discloses determining a usage or purchase mode based on a usage license policy (column 6, line 60-column 7, line 30) and logging data (column 18, lines 53-61), where the log data includes a unique identifier of content data (column 18, lines 53-61), discount information (column 17, lines 35-54, and column 18, lines 53-61), and tracing information (column 18, lines 53-61, and column 6, line 60-column 7, line 46). Christiano further discloses creating usage control status data (column 10, lines 53-57) that includes a content identification (column 10, lines 27-33), the purchase mode (column 10, line 53-column 11, line 11), identification of a circuit module (column 10, lines 33-36), and a user identification (column 10, lines 53-57; column 6, lines 64-column 7, line 1; column 4, line 61-column 5, line 2). Christiano additionally discloses controlling use of content data (column 10, line 64- column 11, line 3) and a usage monitor that monitors the usage control policy and status data to ensure that content data is properly used based on a license (column 6, line 60-column 7, line 46; column 10, lines 53-57). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the apparatus of Schneier by including the usage policies and licensing as disclosed by Christiano, in order to provide a variety of options and flexibility in controlling usage of licensed data (see Christiano, column 3, lines 12-19).

Although Schneier and Christiano disclose a purchase mode (see Christiano, column 10, line 53-column 11, line 11), neither Schneier nor Christiano explicitly discloses that the purchase mode is determined from one or more purchase mode options, each having a different level of restriction imposed on a playback operation.

Stefik discloses a system for controlling distribution and use of digital works that includes a plurality of purchase modes (see Stefik, column 17, line 63-column 26, line 35; more specifically, see column 17, line 64-column 18, line 6; column 19, lines 20-31, describing limitations on number of copies, fees, and times; column 19, lines 46-57, where rights defining playing and printing of a work are described; column 21, lines 10-24, defining limitations on a number of copies to be made; see also column 43, line 45-column 50, line 14, defining various use scenarios) each having a different level of restriction imposed on a playback operation (see again column 17, line 63-column 26, line 35, for a variety of rights, and column 43, line 45-column 50, line 14, for a variety of use scenarios; see also column 36, lines 30-64, where limitations are checked for a playback operation). Stefik also discloses generating log data (column 34, lines 25-34), where the data can include a unique identifier of the content data (column 9, lines 56-66, and Figure 7), discount information (Stefik, column 23, line 44-column 25, line 8), and tracing information (column 48, lines 20-26), and the data can further indicate a result of the determined mode (see again column 17, line 63-column 26, line 35, and column 43, line 45-column 50, line 14, noting, in particular, for example, column 45, lines 33-47). Stefik additionally discloses a public key encryption module (column 26, line 65-column 27, line 9) that performs authentication (column 17, lines 36-47), creates signature data (column 51, lines 9-12), encrypts and decrypts data (column 26, line 65-column 27, line 29), and shares session key data (column 42, lines 6-21), and also discloses a common key encryption module (column 42, lines 6-21) that performs mutual authentication (column 17, lines 36-47) and encrypts and decrypts data with the

session key (column 42, lines 6-21). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the apparatus of Schneier and Christiano by including a plurality of purchase modes each imposing different restrictions on playback, in order to allow the owner of a digital work to attach to the work usage rights defining how the work may be used and/or distributed (see Stefik, column 3, lines 51-61).

Further, although Schneier, Christiano, and Stefik disclose a hash value generating circuit that generates a hash value of content data (Schneier, column 9, lines 40-61; column 17, lines 46-50), none of Schneier, Christiano, or Stefik explicitly discloses also generating a hash value of the key data and usage control policy data. Peinado discloses a system in which a license for digital content includes the content key and usage control policy data (column 2, lines 57-64) and that has a hash value generating circuit that generates a hash value of the content key and policy data and a public key encryption circuit that creates and verifies signature data using the hash (column 2, line 65; column 20, line 38-column 21, line 12). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to further modify the apparatus of Schneier, Christiano, and Stefik, to also compute a hash and generate a signature based on the key and usage policy data, in order to maintain the integrity of those items and prevent alteration of the key or usage policy data and/or prevent unauthorized decryption of content (see Peinado, column 25, lines 53-59) as is well known in the art (see also Schneier, column 9, line 40-column 10, line 67).

8. Claims 18-22 rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier in view of Christiano, Stefik, and Peinado as applied to claim 17 above, and further in view of Castor et al, US Patent 5590288.

In reference to Claims 18 and 19, Schneier as modified above discloses everything as applied to Claim 17 above. However, Schneier as modified above does not explicitly disclose reporting the result of processing by outputting an interrupt. Further, Schneier as modified above does not explicitly disclose that the external bus interface includes a common memory and that the external circuit obtains a result by polling.

Castor discloses a system which allows a computer to request another computer to execute a procedure (column 3, lines 38-42) including outputting an interrupt (column 12, lines 29-33). Castor further discloses a common memory (the buffer of column 12, lines 33-35) and polling an interface circuit to obtain a result (column 12, lines 35-47). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the apparatus of Schneier as modified above by including the interrupt, buffer, and polling of Castor, in order to increase reliability, lower cost, and allow easier upgrades in a distributed computing system (Castor, column 4, lines 11-21).

In reference to Claim 20, Schneier as modified above further discloses first status registers including flags (see Castor, column 12, lines 29-35).

In reference to Claim 21, Schneier as modified above further discloses storing and executing an interrupt program (see Castor, column 5, lines 49-51).

In reference to Claim 22, Schneier as modified above further discloses storing and executing a plurality of interrupt programs and subroutines (see Castor, column 5, lines 49-55).

9. Claim 57 is rejected under 35 U.S.C. 103(a) as being unpatentable over Christiano in view of Stefik and Peinado.

Christiano discloses a method including determining a usage or purchase mode based on a usage license policy (column 6, line 60-column 7, line 30); creating log data (column 18, lines 53-61) that includes a unique identifier of content data (column 18, lines 53-61), discount information (column 17, lines 35-54, and column 18, lines 53-61), and tracing information (column 18, lines 53-61, and column 6, line 60-column 7, line 46).; creating usage control status data (column 10, lines 53-57) that includes a content identification (column 10, lines 27-33), the purchase mode (column 10, line 53-column 11, line 11), identification of a circuit module (column 10, lines 33-36), and a user identification (column 10, lines 53-57; column 6, lines 64-column 7, line 1; column 4, line 61-column 5, line 2); monitoring usage control policy and status data to ensure that content data is properly used based on a license (column 6, line 60-column 7, line 46; column 10, lines 53-57); controlling use of content data (column 10, line 64- column 11, line 3); recording the content data (column 10, lines 62-64, where the product is used on a computer system, and therefore stored at least temporarily therein; see also column 6, lines 28-31, where various storage media are disclosed); performing authentication (column 11, lines 21-30; column 11, line 57-column 12, line 32); and encrypting key

data and control data (column 14, lines 23-28). However, although Christiano discloses a purchase mode (see Christiano, column 10, line 53-column 11, line 11), Christiano does not explicitly disclose that the purchase mode is determined from one or more purchase mode options, each having a different level of restriction imposed on a playback operation, nor does Christiano explicitly disclose creating a signature or sharing a session key.

Stefik discloses a method for controlling distribution and use of digital works that includes a plurality of purchase modes (see Stefik, column 17, line 63-column 26, line 35; more specifically, see column 17, line 64-column 18, line 6; column 19, lines 20-31, describing limitations on number of copies, fees, and times; column 19, lines 46-57, where rights defining playing and printing of a work are described; column 21, lines 10-24, defining limitations on a number of copies to be made; see also column 43, line 45-column 50, line 14, defining various use scenarios) each having a different level of restriction imposed on a playback operation (see again column 17, line 63-column 26, line 35, for a variety of rights, and column 43, line 45-column 50, line 14, for a variety of use scenarios; see also column 36, lines 30-64, where limitations are checked for a playback operation). Stefik also discloses generating log data (column 34, lines 25-34), where the data can include a unique identifier of the content data (column 9, lines 56-66, and Figure 7), discount information (Stefik, column 23, line 44-column 25, line 8), and tracing information (column 48, lines 20-26), and the data can further indicate a result of the determined mode (see again column 17, line 63-column 26, line 35, and column 43, line 45-column 50, line 14, noting, in particular, for example, column 45,

lines 33-47). Stefik additionally discloses performing authentication (column 17, lines 36-47), creating signature data (column 51, lines 9-12), sharing session key data (column 42, lines 6-21), and encrypting data using the session key data (column 42, lines 6-21). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Christiano by including a plurality of purchase modes each imposing different restrictions on playback, in order to allow the owner of a digital work to attach to the work usage rights defining how the work may be used and/or distributed (see Stefik, column 3, lines 51-61).

Further, although Christiano and Stefik generally disclose signature data (Stefik, column 51, lines 9-12), neither Christiano nor Stefik explicitly discloses generating a hash value of the content data, key data, and usage control policy data, or creating signature data using the hash values and then verifying the integrity of the signature data. Peinado discloses a method in which a license for digital content includes the content key and usage control policy data (column 2, lines 57-64), and that the method includes generating a hash value of the content data, content key, and policy data, and creating and verifying signature data using the hash (column 2, line 65; column 20, line 38-column 21, line 12; column 25, lines 41-59). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to further modify the method of Christiano and Stefik to compute a hash and generate a signature based on the key and usage policy data, in order to maintain the integrity of those items and prevent alteration of the key or usage policy data and/or prevent unauthorized decryption of content (see Peinado, column 25, lines 53-59). It would further have been

obvious to include computation of a hash and generation of a signature of the content data itself, in order to prevent alteration of the content data itself (see Peinado, column 25, lines 53-59) as is well known in the art.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571)272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Zachary A Davis/
Examiner, Art Unit 2437